

ANTI MONEY LAUNDERING (AML)

The Anti-Money Laundering (AML) Policy

Is to help prevent officers and members, (including agency workers) from being exposed to the risk of committing an offence relating to money laundering or terrorist financing.

What is Money Laundering

Money laundering is the process by which criminals disguise the origins of property derived from illegal activity, by making it seem to have come from a legitimate source. Typically, this involves repeated movements of the criminal property through a variety of transactions to make it more difficult to trace back to its criminal origins.

Possible Areas of High Risk


Money Laundering can occur over a range of activities, which may not be easy to identify. Here are a few potential examples:

- The existence of a secretive customer who may fail or refuse to provide information when requested without appropriate explanation.
- Payment of a substantial sum in cash, overpayments, or regular/high value refunds.
- The involvement of a 3rd party, without obvious purpose, which appears uneconomic or illogical.
- The supply of a service, where the infiltration of a serious/organised crime group, takes advantage of a public sector contract.
- Movement of funds to/from high-risk countries.




RECORD KEEPING

Once key information has been obtained and verified, activity should be monitored, and documents updated as necessary. Records of identification and business transactions must be kept for at least five years after the transaction or end of the business relationship. All records must be kept in accordance with data protection legislation.



CUSTOMER DUE DILIGENCE


This applies to the regulated sector only, although certain discrete areas of the Council may need to take extra care when obtaining information from the client. Key to this is obtaining appropriate evidence to confirm the identity of the client, and the purpose and intended nature of the business relationship or transaction. Where this is a corporate client, the ownership and control structure, need to be understood. These requirements do not apply to internal clients.



TRAINING


All staff need to be aware of how they may come across money laundering activity in their roles, and what they should do if this happens. For those staff most likely to encounter suspicious activity they also need to be aware of relevant procedures, personal responsibilities and of potential individual liabilities. A free on-line training module is available on PAL.

In line with regulations, the council's arrangements to mitigate against the risk of money laundering are as follows. See full policy for further details.



THE MONEY LAUNDERING REPORTING OFFICER (MLRO)

Where you know or suspect that money laundering activity is taking place or has taken place, then you must report your concerns to the MLRO. The MLRO for the Council is the Head of Audit.



DISCLOSURE PROCEDURE

Complete and submit the AML proforma which is attached to the policy. This will enable the MLRO to make a judgment regarding the potential money laundering activity and the next steps. Do not make any further enquiries yourself or voice any suspicions to the person(s) suspected, or to any other third party. Do not make any reference on the client file. You can only proceed with any relevant transaction(s) once you have received consent from the MLRO.



RISK ASSESSMENTS

Appropriate steps should be taken to identify, assess and understand the money laundering and terrorist financing risks faced by your 'business'. This will help enable you to review the AML measures required to mitigate your risks. Key risks that you should consider include the client, service being delivered, and transaction considerations.



Key Legislation

THE TERRORISM ACT 2000 (TACT) makes it an offence to raise or send funds for suspected terrorists, or to enter into or become concerned in an arrangement relating to the retention or control of property likely to be used for the purposes of terrorism or resulting from acts of terrorism.

PROCEEDS OF CRIME ACT 2002 (POCA): the principal money laundering offences apply to all public authorities and their staff, and include becoming involved in money laundering, acquiring criminal proceeds, and tipping off a suspect about an investigation

THE MONEY LAUNDERING, TERRORIST FINANCING AND TRANSFER OF FUNDS (INFORMATION FOR PAYER) REGULATIONS 2017 AND UPDATES requires regulated firms and those carrying out 'regulated business' only to adopt a risk-based approach to prevent criminals from using their services. Whilst the public sector is not bound by these regulations, there may be some discrete areas of work within the Council to which they may apply. It is best practise for the Council to adhere to them.